On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two

Pantelimon Stănică [*]
Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, USA
E-mail: pstanica@nps.edu

Proc. NATO-Advanced Studies Institute
Boolean Functions in Cryptology and Information Security (Nato Science for Peace and Security) Ed. O.A. Logachev (2008)

Abstract

In this paper we present a result towards the conjectured nonexistence of homogeneous rotation symmetric bent functions having degree > 2.

Keywords. Boolean Functions; Algebraic Normal Form; Nonlinearity; Rotational Symmetry.

1 Introduction

The class of rotation symmetric Boolean functions (RSBFs) has received a lot of attention from a combinatorial and cryptographic perspective [1, 2, 4, 5, 9, 10, 11, 14, 15, 3]. The initial study on the nonlinearity of these functions was done in [4], where nonlinearity was the main focus. Later on, the nonlinearity and correlation immunity of such functions have been studied in detail in [1, 5, 9, 10, 14, 15]. Applications of such functions in hashing has also been investigated [11]. The set of RSBFs are interesting to look into as the space is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space

[*] The author was partially supported by the Naval Postgraduate School RIP funding.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Applied Mathematics,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In this paper we present a result towards the conjectured nonexistence of homogeneous rotation symmetric bent functions having degree > 2.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

of Boolean functions (2^{2^n}) and the set contains functions with very good cryptographic properties. It has been experimentally demonstrated that there are functions in this class which are good in terms of balancedness, nonlinearity, correlation immunity, algebraic degree and algebraic immunity (resistance against algebraic attack) [3] at the same time.

It is interesting to note that the famous Patterson–Wiedemann functions [PW83] that achieve nonlinearity 16276 (strictly greater than nonlinearity $2^{15-1} - 2^{(15-1)/2}$ obtained by bent functions concatenation) in 15 variables are in fact rotation symmetric. Moreover, Kavut et al. [6, 7, 8] proved that there exist rotation symmetric functions in 9 variables having nonlinearity 241 and 242 (which is also strictly greater than the bent concatenation nonlinearity $2^{9-1} - 2^{(9-1)/2}$), which was rather surprising and gives further motivation for the rotation symmetric Boolean functions investigation.

Regarding, the combinatorial structure of these functions, Stănică et al. [15] showed that the Walsh spectra of RSBFs give rise to a certain matrix with interesting combinatorial properties that helps in fast calculations of different cryptographic properties of these functions. Later this matrix has been studied in detail in [9, 10] for odd number of variables and new structures have been discovered. However, the problem remained open for even variable case.

It is well known that bent functions only exist on even number of variables [12]. The rotation symmetric bent functions have been studied in detail in [1, 4, 15, 14]. Here, we present a large class of homogeneous RSBFs which are not bent. This partially answers the conjecture presented in [14].

1.1 Preliminaries

A Boolean function f on n variables may be viewed as a mapping from $\mathbb{F}_2^n = \{0,1\}^n$ into the two-element field $\mathbb{F}_2$; it can also be interpreted as the output column of its *truth table* f, that is, a binary string of length 2^n, $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), \ldots, f(1,1,\cdots,1)]$.

The *Hamming distance* between S_1, S_2 is denoted by $d(S_1, S_2) = \#(S_1 \neq S_2)$. Also the *Hamming weight* or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

The addition operator over $\mathbb{F}_2$ is denoted by $\oplus$. An n-variable Boolean function f can be considered to be a multivariate polynomial over $\mathbb{F}_2$. This polynomial can be expressed as a sum of products representation of all distinct k-th order products ($0 \leq k \leq n$) of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1\leq i\leq n} a_i x_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$. A Boolean function is said to be *homogeneous* if its ANF contains terms of the same degree only.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an n-variable function f is

$$N_f = \min_{g\in A(n)} (d(f, g)),$$

i.e., the distance from the set of all n-variable affine functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belonging to $\mathbb{F}_2^n$ and $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over $\mathbb{F}_2^n$ which is defined as

$$W_f(\omega) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus x\cdot\omega}.$$

In terms of Walsh spectra, the nonlinearity of f is given by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega\in\mathbb{F}_2^n} |W_f(\omega)|.$$

Let $x_i \in \mathbb{F}_2$ for $1 \leq i \leq n$. For $1 \leq k \leq n$, we define the permutation $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k}$, if $i + k \leq n$ and $\rho_n^k(x_i) = x_{i+k-n}$, if $i + k > n$. For $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, we extend the definition by $\rho_n^k(x_1, x_2, \ldots, x_{n-1}, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_{n-1}), \rho_n^k(x_n))$. Hence, ρ_n^k acts as k-cyclic rotation on an n-bit vector.

Definition 1. *A Boolean function f is called* rotation symmetric *if for each input $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$,*

$$f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n) \text{ for } 1 \leq k \leq n.$$

That is, the rotation symmetric Boolean functions are invariant under cyclic rotation of inputs. The inputs of a rotation symmetric Boolean function can be divided into partitions so that each partition consists of all cyclic shifts of one input. A partition is generated by $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \leq k \leq n\}$ and the number of such partitions is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let $\phi(k)$ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see [14]) $g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$.

By $g_{n,w}$ we denote the number of partitions with weight w. For the formula of how to calculate $g_{n,w}$ for arbitrary n and w, we refer to [14, 9, 10].

A *partition*, or *group*, is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the group [15]. These representative elements are again arranged lexicographically. *The rotation symmetric truth table* (RSTT) is defined as the g_n-bit string $[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})]$.

2 The Result

Construction and enumeration of bent RSBFs have been studied in [4, 14, 15, 1]. In [14], it has conjectured that there are no homogeneous bent RSBFs of degree greater than two. Some partial result in this direction has been presented in [15, Theorem 5]. Here we will present another approach which provides a different insight into this problem. Let us now recall [16, Theorem 30].

Theorem 1 (Zheng-Zhang-Imai [16])**.** *Let f be a function on $\mathbb{F}_2^n$ and J be a subset of $\{1, 2, \ldots, n\}$ such that f does not contain any term $x_{j_1} \cdots x_{j_t}$ where $t > 1$ and $j_1, \ldots, j_t \in J$. Then the nonlinearity of f, $N_f \leq 2^{n-1} - 2^{s-1}$, where $s = |J|$.*

As an example, take an 8-variable RSBF f having SANF $x_1x_2x_3$, i.e., the algebraic normal form $x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_7 \oplus x_6x_7x_8 \oplus x_7x_8x_1 \oplus x_8x_1x_2$. Refer to [15, Section 3] for the definition of Short Algebraic Normal Form (SANF). Let $J = \{1, 2, 4, 5, 7\}$ as in the previous theorem. It is easy to see that there is no term in f with *all* indices from J. Since $|J| = 5$, it follows that the nonlinearity $\leq 2^7 - 2^4 = 128 - 16 = 112$; in reality, the nonlinearity is 80.

Next, we present our main result which gives more insight to the mentioned conjecture than [15, Theorem 5]. Theorem 2(iii) supports the conjecture presented in [14] for a large class of homogeneous RSBFs. For a homogeneous degree d RSBF f with its SANF given by $\sum_{i=1}^{s} \beta_i$, where $\beta_i = x_{k_1^{(i)}} x_{k_2^{(i)}} \cdots x_{k_d^{(i)}}$ (note that $k_1^{(i)}$ is 1 for all i), we define a sequence $d_j^{(i)}$, $j = 1, 2, \ldots, k_{i-1}^{(i)}$, by $d_j^{(i)} = k_{j+1}^{(i)} - k_j^{(i)}$. Let $d_f = \max_{i,j}\{d_j^{(i)}\}$, that is, the largest distance between two consecutive indices in all monomials of f.

Theorem 2. *The following hold for a homogeneous RSBF f of degree $d \geq 3$ in n variables:*

(i) *If the SANF of f is $x_1 \ldots x_d$, then f is not bent.*

(ii) *If the SANF of f is $x_1x_2 \ldots x_{d-1}x_d \oplus x_1x_2 \ldots x_{d-1}x_{d+1}$, then f is not bent, assuming: $\frac{n-2}{4} > \lfloor \frac{n}{d} \rfloor$, if $n \not\equiv 1 \pmod{d}$; $\frac{n}{4} > \lfloor \frac{n}{d} \rfloor$, if $n \equiv 1 \pmod{d}$.*

(iii) *In general, if $d_f < \frac{n/2-1}{\lfloor n/d \rfloor}$, then f is not bent.*

Proof. It is easy to check the claim for $n = 6$. Now we consider $d \geq 3$ and $n \geq 8$.

Take the rotation symmetric Boolean function f with SANF $x_1x_2 \ldots x_d$. Assume first that $n \not\equiv 0 \pmod{d}$. Let $J = \{1, 2, \ldots, d-1, d+1, d+2, \ldots, 2d-1, 2d+1, \ldots, \lfloor n/d \rfloor d - 1, \lfloor n/d \rfloor d + 1, \ldots, n-1\}$. Since f is homogeneous and there are no d consecutive indices (assume $x_{n+1} := x_1$, etc.), as required by the terms of f, it follows that the set J satisfies the conditions of Theorem 1. To find the number of elements of J, we count the missing indices, obtaining $|J| = n - \lfloor n/d \rfloor - 1$. Thus, $N_f \leq 2^{n-1} - 2^{n - \lfloor n/d \rfloor - 2}$. Since $d \geq 3$ and $n \geq 8$, then $\lfloor n/d \rfloor + 1 \leq \lfloor n/3 \rfloor + 1 \leq n/3 + 1 < n/2$. Therefore, $n - \lfloor n/d \rfloor - 2 > n/2 - 1$, which implies $N_f < 2^{n-1} - 2^{n/2-1}$, so f is not bent.

If $n \equiv 0 \pmod{d}$, take $J = \{1, 2, \ldots, d-1, d+1, d+2, \ldots, 2d-1, 2d+1, \ldots, \lfloor n/d \rfloor d - 1 = n - 1\}$, with $|J| = n - n/d$. Thus, $N_f \leq 2^{n-1} - 2^{n - \lfloor n/d \rfloor - 1} < 2^{n-1} - 2^{n/2-1}$, so f is not bent, in this case, as well.

We prove next claim (ii) for the homogeneous rotation symmetric Boolean function f with SANF $x_1x_2 \ldots x_d \oplus x_1x_2 \ldots x_{d-1}$. Assume that $n \not\equiv 0, 1 \pmod{d}$. Take $J = \{1, 2, \ldots, d-1, d+2, \ldots, \lfloor n/d \rfloor d - 1, \lfloor n/d \rfloor d + 2, \ldots, n-2\}$, which satisfies Theorem 1, since there are no d consecutive indices with a gap of length 2. By counting missing indices, we obtain $|J| = n - 2\lfloor n/d \rfloor - 1$, therefore $N_f \leq 2^{n-1} - 2^{n - 2\lfloor n/d \rfloor - 2} < 2^{n-1} - 2^{n/2-1}$, if $n/2 - 1 < n - 2\lfloor n/d \rfloor - 2$, which is equivalent to $n > 4\lfloor n/d \rfloor + 2$.

Next, assume that $n \equiv 0 \pmod{d}$, respectively, $n \equiv 1 \pmod{d}$. In these cases, take $J_0 = \{2, \ldots, d-1, d+2, \ldots, \lfloor n/d \rfloor d - 1 = n - 1\}$, respectively, $J_1 = \{1, 2, \ldots, d-1, d+2, \ldots, \lfloor n/d \rfloor d - 1 = n - 2\}$. Both J_0, J_1 satisfy

Theorem 1 and as before, counting missing indices, we obtain $|J_0| = n - 2\lfloor n/d \rfloor - 1$ and $J_1 = n - 2\lfloor n/d \rfloor$. It follows that, under $n \equiv 0 \pmod{d}$, $N_f \leq 2^{n-1} - 2^{n-2\lfloor n/d \rfloor - 2} < 2^{n-1} - 2^{n/2-1}$, if $n/2 - 1 < n - 2\lfloor n/d \rfloor - 2$, which is equivalent to $n > 4\lfloor n/d \rfloor + 2$. Also, under $n \equiv 1 \pmod{d}$, $N_f \leq 2^{n-1} - 2^{n-2\lfloor n/d \rfloor - 1} < 2^{n-1} - 2^{n/2-1}$, if $n/2 - 1 < n - 2\lfloor n/d \rfloor - 1$, which is equivalent to $n > 4\lfloor n/d \rfloor$.

We prove now claim (iii). If $d_f = 1$, it follows that f is generated by $x_1 x_2 \cdots x_d$, and the result follows from part (i). Assume that $d_f \geq 2$.
Case 1. $n \equiv k_0 \pmod{d}$, $k_0 \geq d_f$. We use once again Theorem 1. Take $J_1 = \{d_f, d_f + 1, \ldots, d - 1, d + d_f, d + d_f + 1, \ldots, d\lfloor n/d \rfloor - 1 = n - k_0 - 1, d\lfloor n/d \rfloor + d_f, \ldots, n - 1\}$.
Case 2. $n \equiv k_0 \pmod{d}$, $0 \leq k_0 < d_f$. Take $J_2 = \{d_f - k_0, d_f - k_0 + 1, \ldots, d - 1, d + d_f, d + d_f + 1, \ldots, d\lfloor n/d \rfloor - 1 = n - k_0 - 1\}$.

Both J_1, J_2 satisfy the conditions of Theorem 1 and $|J_1| = n - d_f\lfloor n/d \rfloor - 1$, $|J_2| = n - d_f\lfloor n/d \rfloor$. Therefore, in Case 1, $N_f \leq 2^{n-1} - 2^{n - d_f\lfloor n/d \rfloor - 2} < 2^{n-1} - 2^{n/2-1}$, with the last inequality holding if and only if $n/2 - 1 < n - d_f\lfloor n/d \rfloor - 2$. The last inequality follows from our imposed condition $d_f < \frac{n/2-1}{\lfloor n/d \rfloor}$.

In Case 2, $N_f \leq 2^{n-1} - 2^{n - d_f\lfloor n/d \rfloor - 1} < 2^{n-1} - 2^{n/2-1}$, with the last inequality holding if and only if $n/2 - 1 < n - d_f\lfloor n/d \rfloor - 1$. The last inequality follows from $d_f < \frac{n/2-1}{\lfloor n/d \rfloor} < \frac{n/2}{\lfloor n/d \rfloor}$. □

References

[1] J. Clark, J. Jacob, S. Maitra and P. Stănică. Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. *Computational Intelligence*, Pages 450–462, Volume 20, Number 3, 2004.

[2] T. W. Cusick and P. Stănică. Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions. *Discrete Mathematics* **258**, 289–301, 2002.

[3] D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *Progress in Cryptology - INDOCRYPT 2004*, to be published in Lecture Notes in Computer Science, Springer-Verlag.

[4] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*, Springer-Verlag, 1998.

[5] M. Hell, A. Maximov and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. In *Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004*, June 19–25, 2004, Black Sea Coast, Bulgaria.

[6] S. Kavut, S. Maitra and M. D. Yücel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240, Indocrypt 2006 (Berlin: Springer LNCS 4329, 2006), 266–279.

[7] S. Kavut, S. Maitra and M. D. Yücel. Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class, *IEEE Trans. Inform. Theory* 53 (2007), 1743–1751.

[8] S. Kavut and M. D. Yücel. Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions - 9 variable Boolean Functions with Nonlinearity 242, to appear in Proc. of AAECC 2007.

[9] A. Maximov, M. Hell and S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. IACR eprint server, eprint.iacr.org, no. 2004/144, 2004.

[10] A. Maximov. Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra. IACR eprint server, no. 2004/354.

[PW83] N. J. Patterson and D. H. Wiedemann The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276, *IEEE Trans. Inform. Theory* 29 (1983), 354-356; See also the correction in *IEEE Trans. Inform. Theory* 36 (1990), 443.

[11] J. Pieprzyk and C. X. Qu. Fast Hashing and Rotation-Symmetric Functions. *Journal of Universal Computer Science* **5**, 20–31, 1999.

[12] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, pages 300–305, vol 20, 1976.

[13] P. Savicky. On the bent Boolean functions that are symmetric. *European Journal of Combinatorics*, 15:407–410, 1994.

[14] P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, December 2002. Electronic Notes in Discrete Mathematics, Elsevier, Vol 15. The extended version will appear in *Discrete Applied Mathematics*, 2008.

[15] P. Stănică, S. Maitra and J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. *Fast Software Encryption Workshop (FSE 2004)*, New Delhi, INDIA, LNCS **3017**, Springer Verlag, 161–177, 2004.

[16] Y. Zheng, X-M. Zhang and H. Imai. Restriction, terms and nonlinearity of Boolean functions. *Theoretical Computer Science*, 226:207–223, 1999.